

UNIVERSIDADE da MADEIRA

CTeSP

CURSOS TÉCNICOS
SUPERIORES PROFISSIONAIS

RELATÓRIO

RELATÓRIO DO PROJETO DE SEGURANÇA INFORMÁTICA

Miguel Peñaranda N°2019122

Curso Técnico Superior Profissional em
Tecnologias e Programação de Sistemas de
Informação

UNIDADE CURRICULAR:

Segurança Informática

DOCENTE:

Lisandro Marote

DATA:

20 de janeiro de 2024

ESCOLA SUPERIOR DE TECNOLOGIAS E GESTÃO

ÍNDICE

1. INTRODUÇÃO	5
2. DESENVOLVIMENTO	6
• Etapa 1	6
• Etapa 2	6
• Etapa 3	7
Tabela de Endereçamento da Rede	7
• Etapa 4	8
• Etapa 5	9
• Etapa 6	10
• Etapa 7	10
• Etapa 8	11
• Etapa 9	12
• Etapa 10	12
• Etapa 11	14
Criar uma ACL que negue todo o tráfego entre as LANs do R1 e do R3	14
Todo o tráfego da rede local do R3 com destino à porta TCP 80, 443 e DNS deve ser permitido ...	15
A Rede do R3 deverá poder comunicar em FTP para as LAN dos R4 e R6	15
Qualquer tráfego não especificado deve ser negado	16
• Etapa 12	16
Zona Outside:	16
Zona Inside:	17
Zona DMZ:	17
• Etapa 13	19
• Etapa 14	19
3. CONCLUSÃO	21

Ilustração 1 - Topologia da Rede	6
Ilustração 2 - Banner Configurado em Todos os Dispositivos de Rede	7
Ilustração 3 - Verificação do Funcionamento das Rotas Estáticas	9
Ilustração 4 - Verificação do Mínimo de Caracteres nas Senhas	10
Ilustração 5 - Enable Secret "cisco12345"	10
Ilustração 6 - Utilizador Criado em Todos os Routers e Switchs	10
Ilustração 7 - Ligação a um Router desde o PC-A	11
Ilustração 8 - Tentativa de Ligação a um Router desde outro PC	11

Ilustração 9 - Criação do Servidor RADIUS	12
Ilustração 10 - Autenticação através do Servidor RADIUS no R1	13
Ilustração 11 - Autenticação através do Servidor RADIUS no R3	13
Ilustração 12 - Verificação de que a ACL foi Implementada com Sucesso I	14
Ilustração 13 - Verificação de que a ACL foi Implementada com Sucesso II	14
Ilustração 14 - Verificação do Tráfego Permitido através da porta TCP 80, 443 e DNS	15
Ilustração 15 - Ligação ao Servidor da LAN R4 através de FTP com Sucesso	15
Ilustração 16 - Negação de Tráfego não Especificado	16
Ilustração 17 - Nenhum Tráfego Iniciado na Zona Outside é Permitido para a Rede Interna	17
Ilustração 18 - Ligação do PC-B ao PC-D através de HTTP	18
Ilustração 19 - Ligação desde o PC-F ao PC-B através de HTTP	18
Ilustração 20 - Nenhum Tráfego é Permitido Entre a Rede Interna e a DMZ	19
Ilustração 21 - Verificação do Encaminhamento de Pacotes através do Túnel IPsec desde o R4	20
Ilustração 22 - Verificação do Encaminhamento de Pacotes através do Túnel IPsec desde o R6	20

AGRADECIMENTOS

Para iniciar, quero agradecer ao docente Lisandro Marote, que fez um grande esforço em nos ensinar o conteúdo necessário para nos adentrar no mundo da segurança informática, sempre estive disposto para esclarecer as nossas dúvidas e para motivar-nos a desenvolver os conhecimentos adquiridos durante as aulas.

1. INTRODUÇÃO

No relatório a seguir, será apresentado o nosso projeto proposto pelo professor Lisandro Marote para a disciplina de “Segurança Informática”, que consiste na criação uma topologia de uma rede com 7 routers, 4 switches, 3 servidores e 3 PC’s.

Para dar um breve conceito, a segurança informática é uma peça fundamental na preservação da integridade, confidencialidade e disponibilidade dos dados em ambientes tecnológicos.

Desde modo, o presente relatório aborda uma série de etapas cruciais para fortalecer a segurança de uma infraestrutura de rede, garantindo a proteção dos sistemas e dados envolvidos. Isto é através de etapas como a atribuição de nomes aos equipamentos até a ativação de serviços de segurança avançados, cada etapa contribui para a criação de uma rede robusta e resiliente. Enfim ao abordar aspetos como configuração de IPs, implementação de firewalls e protocolos de segurança, o relatório visa fornecer uma visão abrangente das medidas tomadas para mitigar possíveis ameaças e ataques.

2. DESENVOLVIMENTO

- **Etapa 1**

Na primeira etapa a prioridade foi a atribuição adequada de nomes aos equipamentos. A nomenclatura consistente é uma prática essencial para facilitar a identificação e a manutenção dos dispositivos em uma rede. Nesta etapa, cada dispositivo foi nomeado de forma a refletir sua função e localização na topologia de rede.

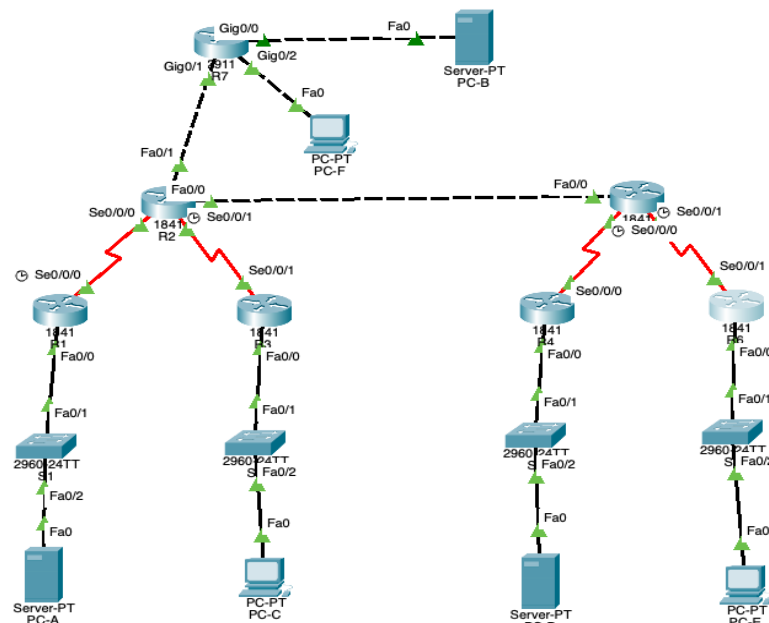


Ilustração 1 - Topologia da Rede

- **Etapa 2**

A segunda envolveu a configuração de banners nos dispositivos da rede. Por tanto, os banners são mensagens informativas exibidas ao acessar um dispositivo, servindo como uma medida adicional para comunicar políticas de segurança ou informações importantes aos utilizadores.

Esta etapa é muito importante porque promove a transparência ao informar aos utilizadores sobre as políticas de segurança em vigor e atuam como uma camada adicional de dissuasão contra acessos não autorizados.

```
*****
*
*      Acesso Restrito - Autorizado
*      Apenas pessoal autorizado pode acessar
*
*      Aluno: Miguel Penaranda
*      N 2019122
*
*****
```

Ilustração 2 - Banner Configurado em Todos os Dispositivos de Rede

- **Etapa 3**

A terceira etapa concentrou-se na configuração dos endereços IP nos dispositivos da rede. Desta forma a atribuição adequada de IPs é essencial para garantir a conectividade e a comunicação eficiente entre os dispositivos.

Tabela de Endereçamento da Rede

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway padrão
R1	Fa0/0	192.28.1.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
R2	Fa0/0	10.3.3.1	255.255.255.252	N/D
	Fa0/1	10.6.6.2	255.255.255.252	N/D
	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
	Loopback 0	62.48.16.12	255.255.255.0	N/D
R3	Fa0/0	192.28.2.1	255.255.255.0	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
R4	Fa0/0	192.28.3.1	255.255.255.0	N/D
	S0/0/0	10.4.4.1	255.255.255.252	N/D

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway padrão
R5	Fa0/0	10.3.3.2	255.255.255.252	N/D
	S0/0/0	10.4.4.2	255.255.255.252	N/D
	S0/0/1	10.5.5.2	255.255.255.252	N/D
R6	Fa0/0	192.28.4.1	255.255.255.0	N/D
	S0/0/1	10.5.5.1	255.255.255.252	N/D
R7	G0/0	172.16.1.1	255.255.255.0	N/D
	G0/1	10.6.6.1	255.255.255.252	N/D
	G0/2	192.28.5.1	255.255.255.0	N/D
PC-A	Fa0	192.28.1.10	255.255.255.0	192.28.1.1
PC-B	Fa0	172.16.1.10	255.255.255.0	172.16.1.1
PC-C	Fa0	192.28.2.10	255.255.255.0	192.28.2.1
PC-D	Fa0	192.28.3.10	255.255.255.0	192.28.3.1
PC-E	Fa0	192.28.4.10	255.255.255.0	192.28.4.1
PC-F	Fa0	192.28.5.10	255.255.255.0	192.28.5.1

• **Etapa 4**

Na quarta etapa do projeto de segurança informática, o foco foi na configuração de rotas estáticas nos dispositivos para permitir a comunicação entre eles. Desde modo as rotas estáticas são essenciais para direcionar o tráfego de maneira eficiente, especialmente em redes pequenas ou em cenários específicos.

As razões para a configuração de rotas estáticas são:

- **Direcionamento de Tráfego**: As rotas estáticas indicam aos dispositivos por qual interface ou gateway enviar pacotes de dados para alcançar redes específicas.
- **Estabelecimento de Conectividade**: Permitem a comunicação eficiente entre redes, direcionando o tráfego para o destino apropriado.

Por tanto a configuração de rotas estáticas é crucial para garantir que os dispositivos na rede possam se comunicar eficientemente. Visto que, ao direcionar o tráfego por meio de rotas específicas, estabelecem uma base sólida para futuras implementações de segurança e gerenciamento de rede.

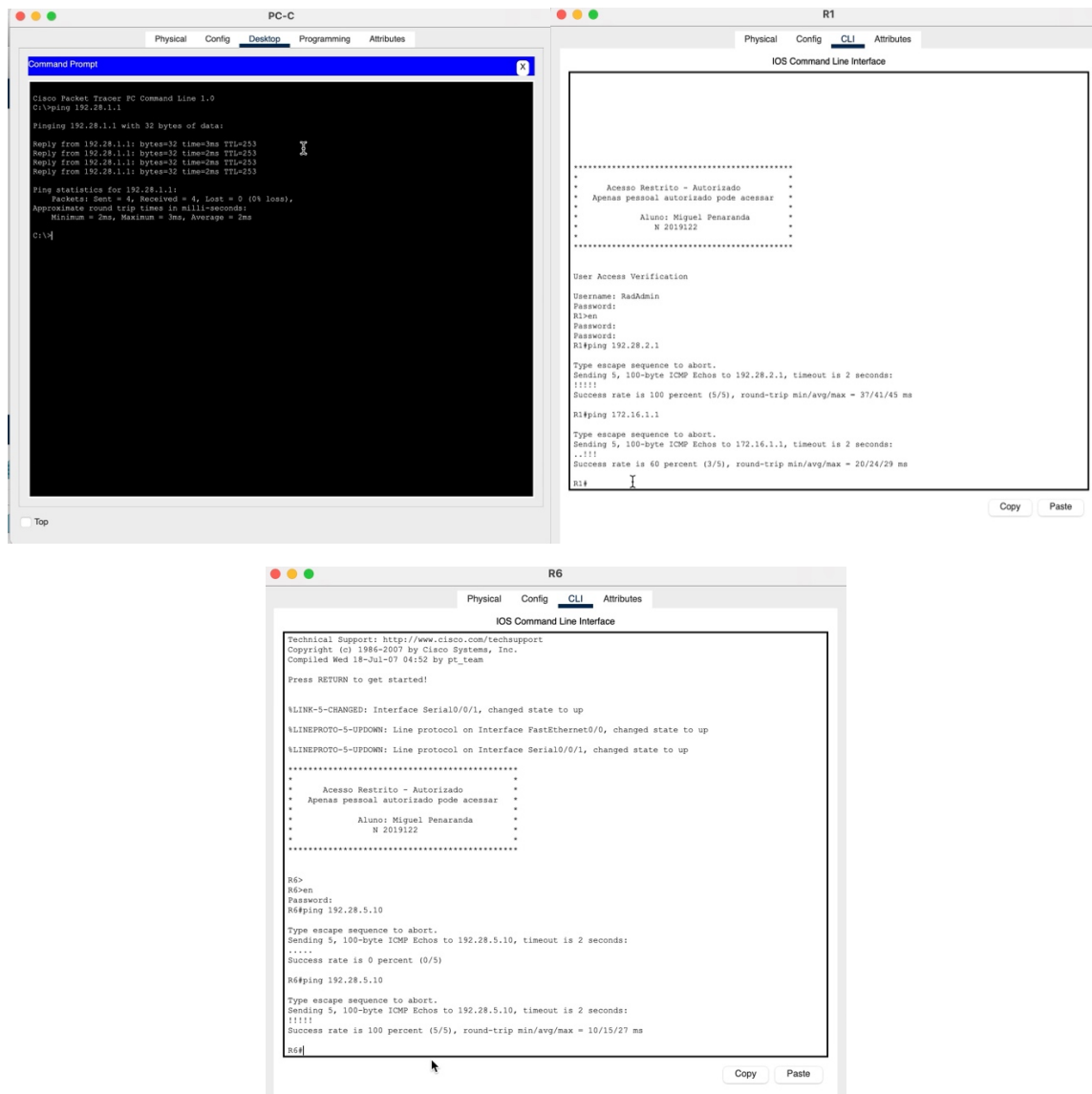


Ilustração 3 - Verificação do Funcionamento das Rotas Estáticas

• **Etapa 5**

Na quinta etapa estabeleceu-se a configuração de senhas com um tamanho mínimo de 10 caracteres nos dispositivos da rede. Essa prática é fundamental para fortalecer a segurança, tornando mais difícil para usuários não autorizados comprometerem as credenciais.

```
*****
*
*      Acesso Restrito - Autorizado      *
*      Apenas pessoal autorizado pode acessar      *
*
*      Aluno: Miguel Penaranda      *
*      N 2019122      *
*
*****

R4>en
Password:
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#user
R4(config)#username ?
WORD User name
R4(config)#username jacky ?
password Specify the password for the user
privilege Set user privilege level
secret Specify the secret for the user
<cr>
R4(config)#username jacky se
R4(config)#username jacky secret ?
0 Specifies an UNENCRYPTED secret will follow
5 Specifies a HIDDEN secret will follow
LINE The UNENCRYPTED (cleartext) user secret
R4(config)#username jacky secret carro
% Password too short - must be at least 10 characters. Password not configured.
R4(config)#
```

Ilustração 4 - Verificação do Mínimo de Caracteres nas Senhas

- **Etapa 6**

Na sexta etapa realizei a configuração da senha de enable nos dispositivos da rede. A senha de enable é crucial para acessar os modos privilegiados de configuração, garantindo a segurança e o controle de acesso aos recursos críticos do dispositivo.

```
!
!
!
enable secret 5 $1$mERr$WvpW0n5TghRrqrwXCUU1.
!
!
```

Ilustração 5 - Enable Secret "cisco12345"

- **Etapa 7**

Na sétima etapa configurei um utilizador com privilégios 15 em todos os roteadores e switches. Além disso, estabeleci a configuração na linha VTY para permitir acesso remoto via SSH.

```
:
!
!
username miguel28 privilege 15 secret 5 $1$mERr$j4iy8dV6b13svO6UkFLFs1
!
!
```

Ilustração 6 - Utilizador Criado em Todos os Routers e Switchs

- **Etapa 8**

Na oitava etapa do projeto de segurança informática, configurei ACL's em todos os roteadores para permitir o acesso remoto apenas pelo PC-A. Assim sendo restringido o acesso através do protocolo ssh aos routers apenas para um dispositivo.

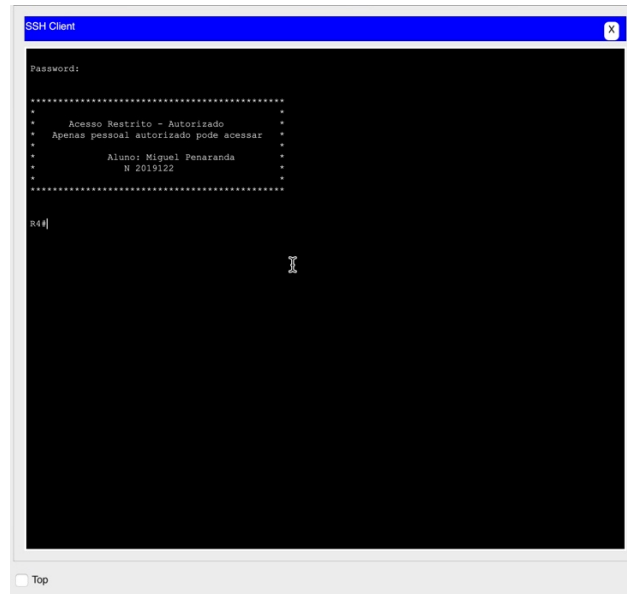


Ilustração 7 - Ligação a um Router desde o PC-A

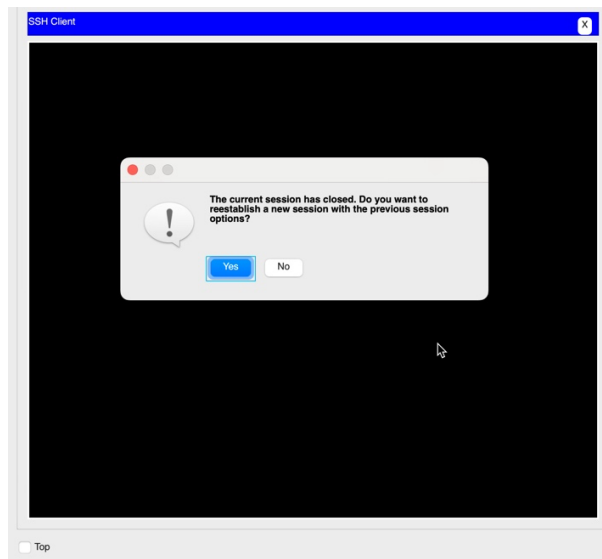
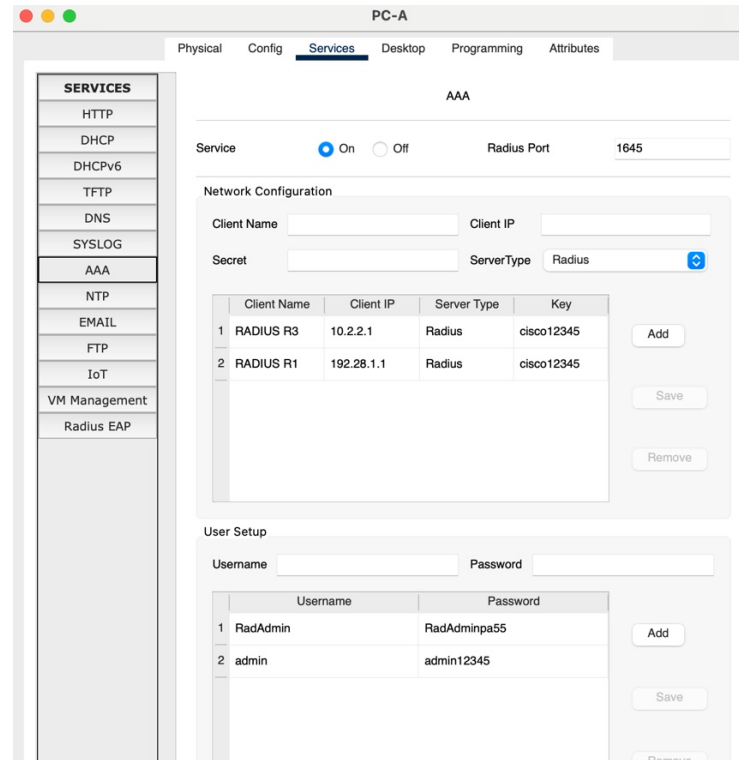


Ilustração 8 - Tentativa de Ligação a um Router desde outro PC

- **Etapa 9**

Na nona etapa configurei um servidor RADIUS no PC-A e criei um utilizador chamado "RadAdmin" com a senha "RadAdminpa55". O RADIUS (Remote Authentication Dial-In User Service) é um protocolo comumente usado para autenticação, autorização e contabilidade em redes.



The screenshot shows the configuration interface for PC-A, specifically the 'Services' tab. The 'AAA' service is selected in the left sidebar. The main configuration area is divided into three sections: Service, Network Configuration, and User Setup.

Service: The 'Service' is set to 'On' (radio button selected). The 'Radius Port' is set to '1645'.

Network Configuration: This section contains fields for 'Client Name', 'Client IP', 'Secret', and 'ServerType'. Below these fields is a table with two entries:

	Client Name	Client IP	Server Type	Key
1	RADIUS R3	10.2.2.1	Radius	cisco12345
2	RADIUS R1	192.28.1.1	Radius	cisco12345

Buttons for 'Add', 'Save', and 'Remove' are located to the right of the table.

User Setup: This section contains fields for 'Username' and 'Password'. Below these fields is a table with two entries:

	Username	Password
1	RadAdmin	RadAdminpa55
2	admin	admin12345

Buttons for 'Add', 'Save', and 'Remove' are located to the right of the table.

Ilustração 9 - Criação do Servidor RADIUS

- **Etapa 10**

Na décima etapa criei um modelo AAA (Autenticação, Autorização e Contabilidade) nos roteadores R1 e R3. Desde modo, o modelo AAA foi configurado com dois métodos de autenticação: o primeiro utilizando o servidor RADIUS no PC-A e o segundo utilizando a base de dados local do roteador.

Por tanto ao criar um modelo AAA nos roteadores R1 e R3 com dois métodos de autenticação, fornecemos redundância e garantimos a disponibilidade contínua da autenticação, mesmo em cenários de falha do servidor RADIUS.

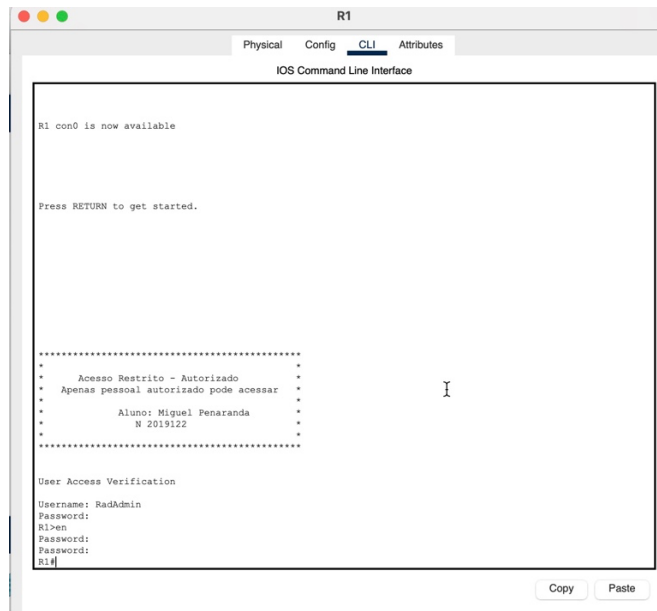


Ilustração 10 - Autenticação através do Servidor RADIUS no R1

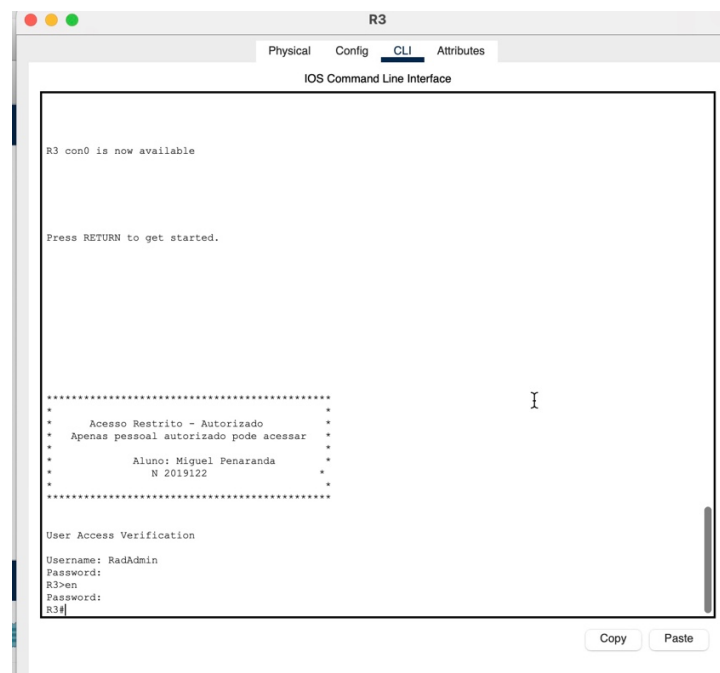


Ilustração 11 - Autenticação através do Servidor RADIUS no R3

- **Etapa 11**

Na décima primeira etapa implementei ACL's para cumprir com as premissas especificadas:

Criar uma ACL que negue todo o tráfego entre as LANs do R1 e do R3

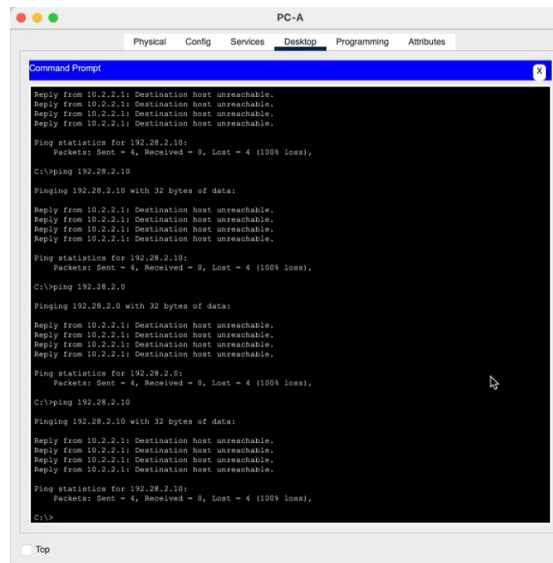


Ilustração 12 - Verificação de que a ACL foi Implementada com Sucesso I

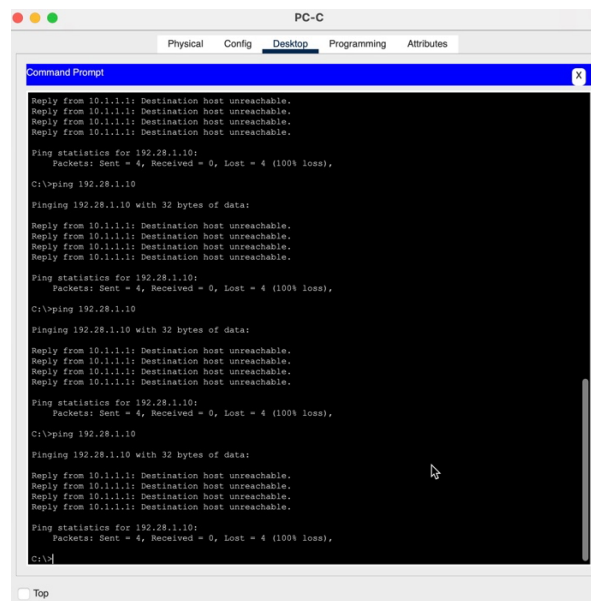


Ilustração 13 - Verificação de que a ACL foi Implementada com Sucesso II

Todo o tráfego da rede local do R3 com destino à porta TCP 80, 443 e DNS deve ser permitido

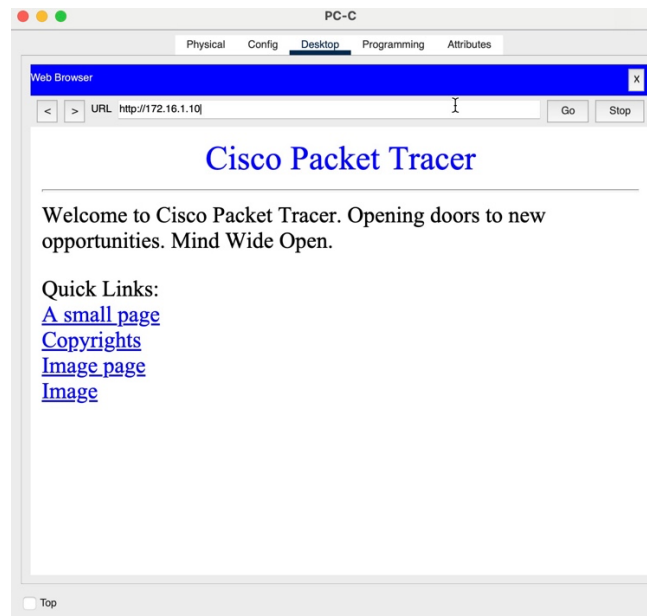


Ilustração 14 - Verificação do Tráfego Permitido através da porta TCP 80, 443 e DNS

A Rede do R3 deverá poder comunicar em FTP para as LAN dos R4 e R6

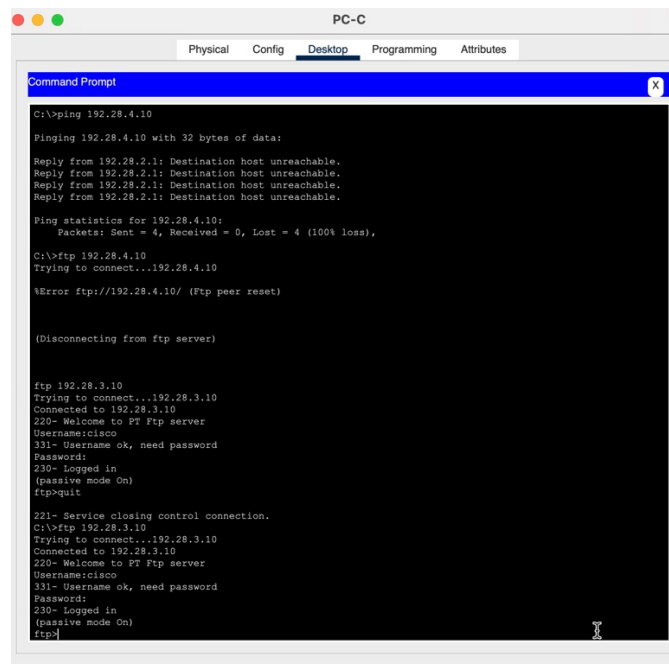
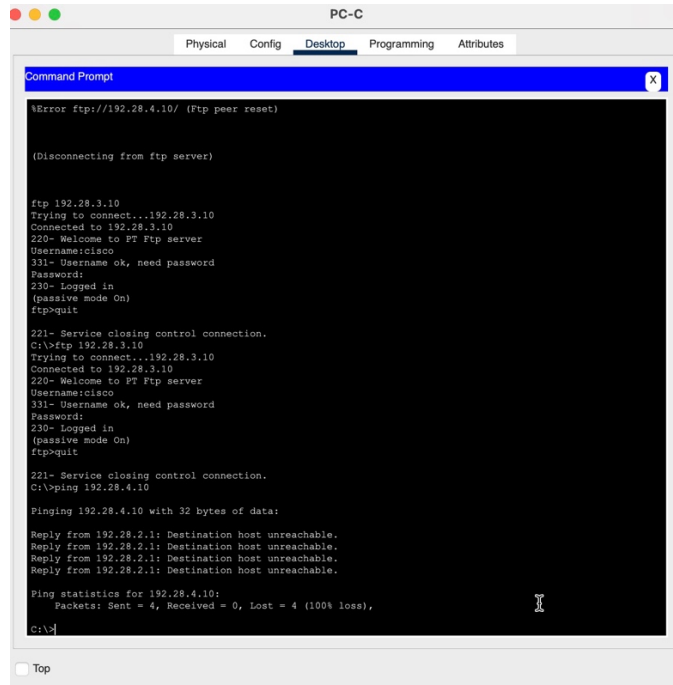


Ilustração 15 - Ligação ao Servidor da LAN R4 através de FTP com Sucesso

Qualquer tráfego não especificado deve ser negado



```
PC-C
Physical Config Desktop Programming Attributes
Command Prompt
%Error ftp://192.28.4.10/ (Ftp peer reset)

(Disconnecting from ftp server)

ftp 192.28.3.10
Trying to connect...192.28.3.10
Connected to 192.28.3.10
220- Welcome to PT Ptp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>ftp 192.28.3.10
Trying to connect...192.28.3.10
Connected to 192.28.3.10
220- Welcome to PT Ptp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>ping 192.28.4.10

Pinging 192.28.4.10 with 32 bytes of data:

Reply from 192.28.2.1: Destination host unreachable.
Reply from 192.28.2.1: Destination host unreachable.
Reply from 192.28.2.1: Destination host unreachable.
Reply from 192.28.2.1: Destination host unreachable.

Ping statistics for 192.28.4.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Ilustração 16 - Negação de Tráfego não Especificado

- **Etapa 12**

Na décima segunda etapa implementei uma Zone-Based Firewall no roteador R7, dividindo a rede em três zonas distintas: Outside, DMZ e Inside. Deste modo a configuração visa atender a premissas especificadas para garantir a segurança e controlar o tráfego entre as zonas.

Zona Outside:

- Todo tráfego iniciado na zona Outside com destino à rede interna é negado, reforçando a segurança da rede interna.
- Permite o tráfego de retorno da zona Outside para o R7, essencial para receber respostas de solicitações originadas de qualquer rede do R7.

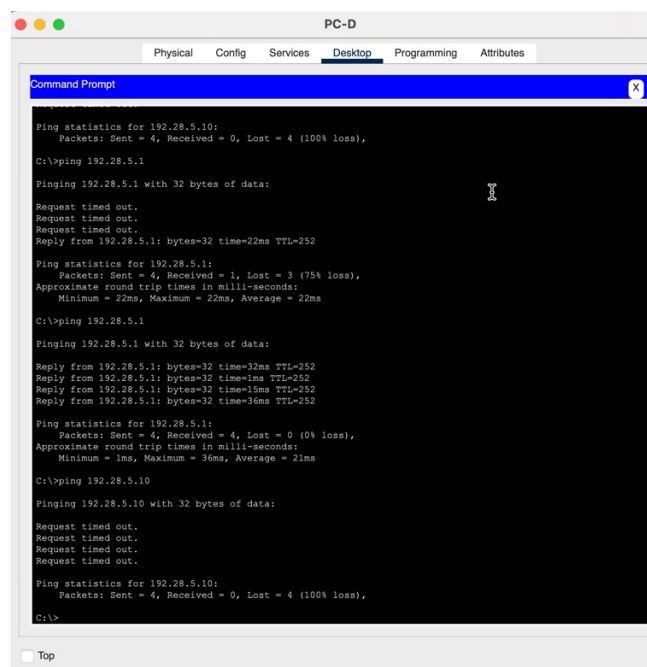
Zona Inside:

- Computadores na rede interna (Inside) têm permissão para iniciar qualquer tipo de tráfego, seja TCP, UDP ou ICMP, reconhecendo-os como confiáveis.
- Implementa uma política rigorosa de segurança ao negar qualquer tráfego direto entre a rede interna e a DMZ.

Zona DMZ:

- Servidores na DMZ têm permissão para iniciar apenas tráfego da Web, limitando-se a HTTP ou HTTPS, contribuindo para um ambiente mais seguro.
- Apenas permite que servidores na DMZ recebam tráfego da Web (HTTP ou HTTPS) proveniente da zona Outside.

Estas configurações de Zone-Based Firewall criam um perímetro robusto de segurança, controlando estritamente o tráfego entre zonas e permitindo apenas as comunicações necessárias para as operações da rede. Por tanto esta abordagem reforça a proteção contra ameaças externas e contribui para um ambiente de rede mais seguro e controlado.



```
PC-D
Physical Config Services Desktop Programming Attributes
Command Prompt

Ping statistics for 192.28.5.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.28.5.1

Pinging 192.28.5.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Reply from 192.28.5.1: bytes=32 time=22ms TTL=252

Ping statistics for 192.28.5.1:
Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 22ms, Average = 22ms

C:\>ping 192.28.5.1

Pinging 192.28.5.1 with 32 bytes of data:

Reply from 192.28.5.1: bytes=32 time=32ms TTL=252
Reply from 192.28.5.1: bytes=32 time=1ms TTL=252
Reply from 192.28.5.1: bytes=32 time=15ms TTL=252
Reply from 192.28.5.1: bytes=32 time=36ms TTL=252

Ping statistics for 192.28.5.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 36ms, Average = 21ms

C:\>ping 192.28.5.10

Pinging 192.28.5.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.28.5.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Ilustração 17 - Nenhum Tráfego Iniciado na Zona Outside é Permitido para a Rede Interna

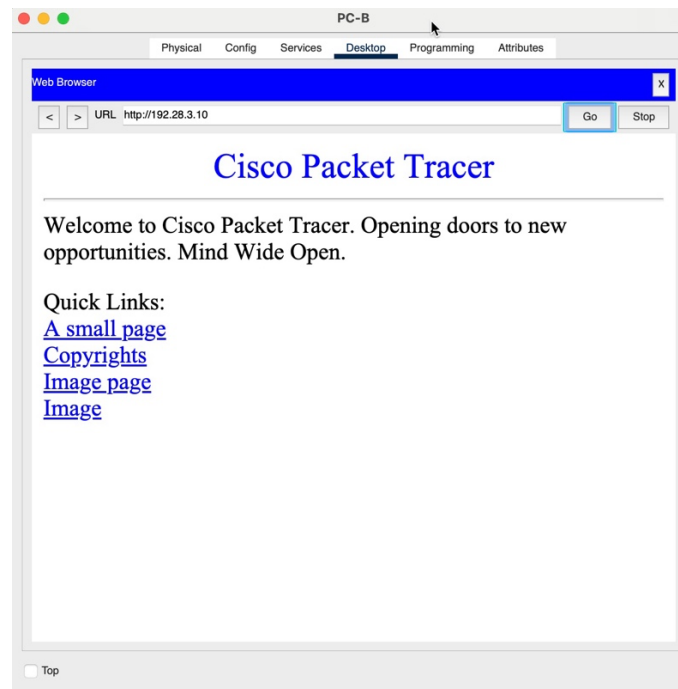


Ilustração 18 - Ligação do PC-B ao PC-D através de HTTP

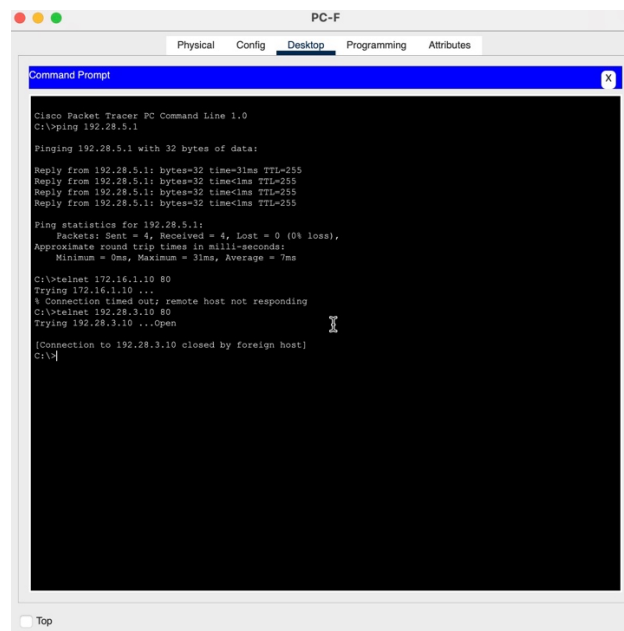


Ilustração 19 - Ligação desde o PC-F ao PC-B através de HTTP

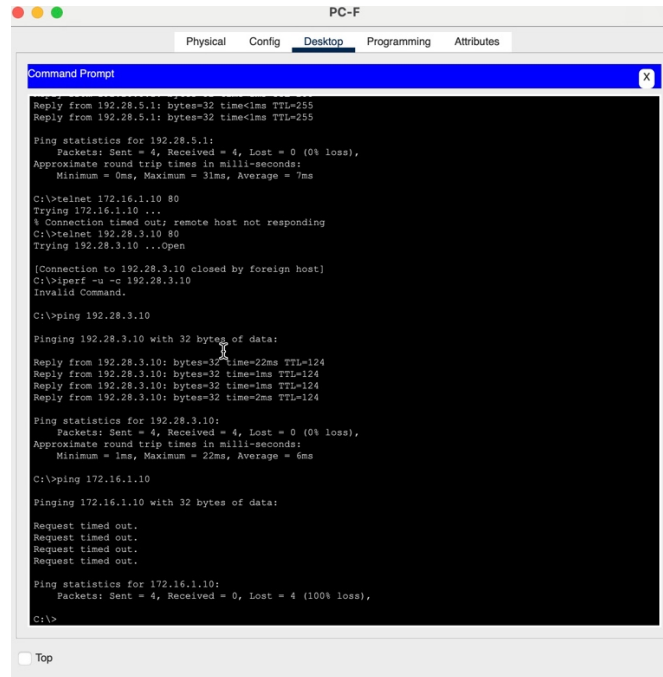


Ilustração 20 - Nenhum Tráfego é Permitido Entre a Rede Interna e a DMZ

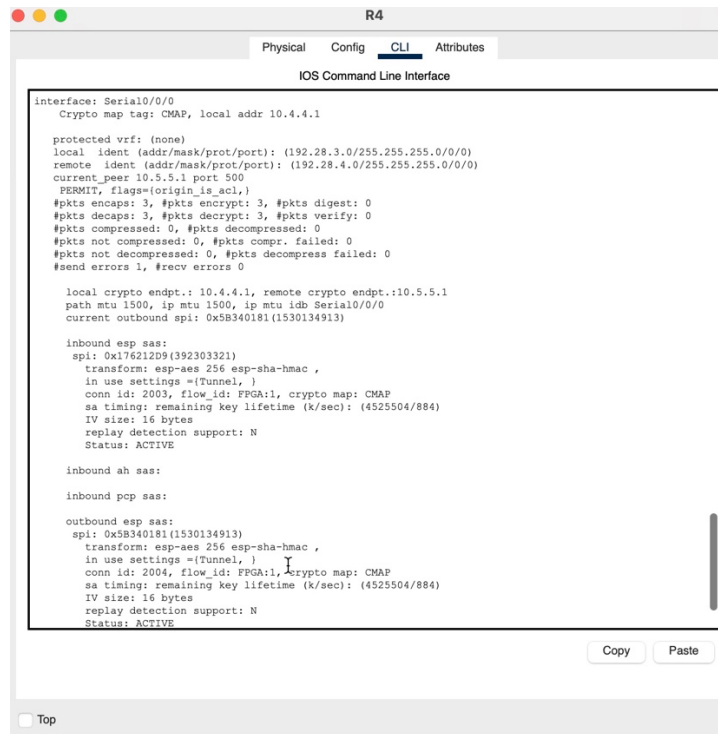
- **Etapa 13**

Na décima terceira etapa implementei a ativação da IPS no Roteador R2 com assinaturas básicas para a rede 10.3.3.0/30 que contribui para a segurança proativa, detectando e mitigando intrusões em tempo real. Além disso, o encaminhamento de logs para o PC-A permite uma análise eficiente das atividades da IPS.

- **Etapa 14**

Na décima quarta etapa configurei um túnel IPSec entre os roteadores R4 e R6 para estabelecer uma comunicação segura entre as LANs associadas a esses dispositivos.

Por tanto a configuração bem-sucedida do túnel IPSec entre R4 e R6 estabelece uma conexão segura entre as respectivas LANs, garantindo a confidencialidade e integridade dos dados transmitidos.



```

R4
Physical Config CLI Attributes
IOS Command Line Interface

interface Serial0/0/0
Crypto map tag: CMAP, local addr 10.4.4.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.28.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.28.4.0/255.255.255.0/0/0)
current_peer 10.5.5.1 port 500
PERMIT, flags=(origin_is_acl,)
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.4.4.1, remote crypto endpt.: 10.5.5.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x5B340181(1530134913)

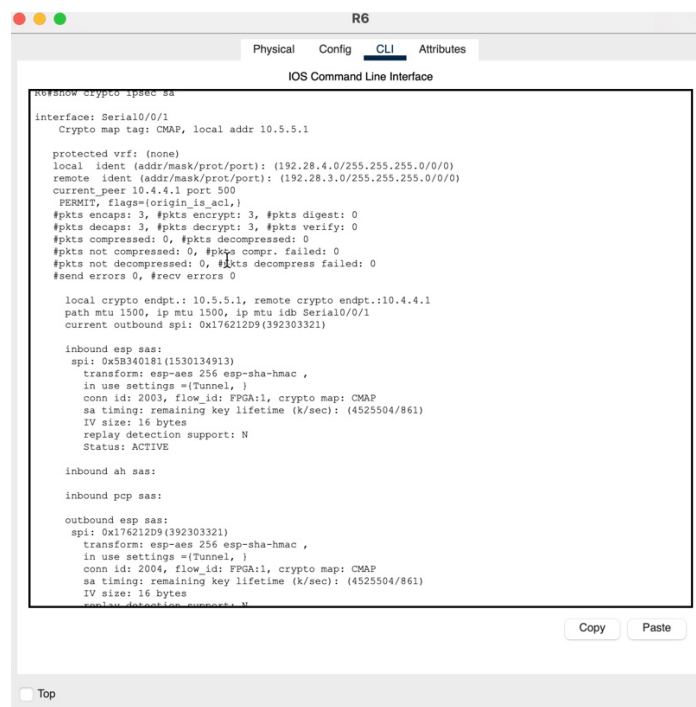
inbound esp sas:
spi: 0x176212D9(392303321)
transform: esp-aes 256 esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 2003, flow_id: FPGA:1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/884)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0x5B340181(1530134913)
transform: esp-aes 256 esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 2004, flow_id: FPGA:1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/884)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
  
```

Ilustração 21 - Verificação do Encaminhamento de Pacotes através do Túnel IPsec desde o R4



```

R6
Physical Config CLI Attributes
IOS Command Line Interface

show crypto ipsec sa

interface Serial0/0/1
Crypto map tag: CMAP, local addr 10.5.5.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.28.4.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.28.3.0/255.255.255.0/0/0)
current_peer 10.4.4.1 port 500
PERMIT, flags=(origin_is_acl,)
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.5.5.1, remote crypto endpt.: 10.4.4.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
current outbound spi: 0x176212D9(392303321)

inbound esp sas:
spi: 0x5B340181(1530134913)
transform: esp-aes 256 esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 2003, flow_id: FPGA:1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/861)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0x176212D9(392303321)
transform: esp-aes 256 esp-sha-hmac ,
in use settings =(Tunnel, )
conn id: 2004, flow_id: FPGA:1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/861)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
  
```

Ilustração 22 - Verificação do Encaminhamento de Pacotes através do Túnel IPsec desde o R6

3. CONCLUSÃO

Em suma, durante o processo de desenvolvimento da topologia especificada, tive a oportunidade de me questionar e tomar decisões fundamentadas nos conhecimentos adquiridos na disciplina de Segurança Informática, melhorando assim as minhas habilidades neste âmbito. Deste modo, durante este projeto, consegui aplicar os conceitos e princípios aprendidos na disciplina, utilizando medidas organizadas e eficientes para a proteção dos sistemas de informação.

Para concluir, o propósito de todas estas etapas foi estabelecer uma infraestrutura de rede robusta e segura. Desde a configuração inicial dos equipamentos, a implementação de práticas de segurança em diversos níveis até a ativação de serviços específicos, cada etapa visa fortalecer a integridade, confidencialidade e disponibilidade da rede. Isto é através da implementação de tecnologias como VPNs, firewalls, IPSec, autenticação segura e serviços de segurança do IOS que visam mitigar ameaças potenciais, proteger dados sensíveis e proporcionar uma comunicação eficaz e segura entre os dispositivos da rede. Por fim ao integrar medidas de segurança em todos os níveis, o resultado é um ambiente de rede resiliente que é capaz de enfrentar desafios de segurança de forma proativa.